Ethical hacking lab: Buff HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

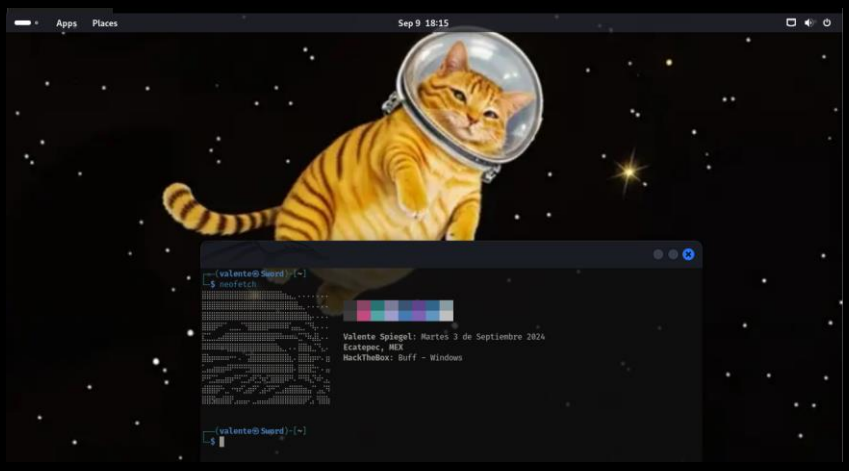
/▲\ Correo /▲\ tiktok /▲\ github

Atacante ---------- |10.10.19.30|

|>/////////// Linux|

Victima ---------- |10.10.11.130|

|> /////// Windows|



Walkthrough

| 1 |

Con un escaneo de puertos utilizando **Nmap**, identificamos un servicio **HTTP** en el puerto **8080**, que revela la ejecución de **Gym Management System 1.0**. Según **Searchsploit**, esta versión presenta una vulnerabilidad de **Ejecución Remota de Comandos (RCE) sin autenticación**. Para explotarla, inyectamos un archivo con doble extensión.**php.png**, aprovechando la función shell_exec de PHP para ejecutar comandos en el sistema.

| 2 |

A continuación, iniciamos un **servidor SMB** en nuestra máquina atacante, donde compartimos los binarios **netcat.exe**, **winPEASx64.exe** y **chisel.exe**. Usamos el binario de **netcat** para establecer una **reverse shell** interactiva, logrando acceso bajo el usuario buff/shaun. Esto nos permite ejecutar **winPEAS**, lo que revela la presencia del servicio **CloudMe 1.1.2** en el puerto **8888**, que no era visible en el escaneo inicial con Nmap.

| 3 |

Utilizando nuevamente **Searchsploit**, descubrimos que **CloudMe** es vulnerable a un **buffer overflow**, lo que nos brinda la oportunidad de sobrescribir el registro **EIP**.

| 4 |

Para preparar el ataque, configuramos un entorno de prueba en un laboratorio local con **Windows 7 Pro**, donde ejecutamos **CloudMe 1.1.2** y desarrollamos un script en **Python** que explota la vulnerabilidad. Usando **Immunity Debugger**, confirmamos que es posible manipular los registros de la pila. A partir de esto, creamos una lista de caracteres controlados utilizando **Metasploit** para identificar la posición exacta donde inyectar el payload. Finalmente, generamos el payload con **msfvenom** en lenguaje C para obtener una **reverse shell** con privilegios de administrador.

| 5 |

Con todo listo, usamos **Chisel** para realizar un **port forwarding** del puerto **8888** de la máquina víctima hacia nuestra máquina atacante. Nos ponemos en escucha en el puerto redirigido y ejecutamos el exploit. El **buffer overflow** se desencadena con éxito, permitiéndonos escalar privilegios y obtener control total del sistema con permisos de administrador.

Habilidades.

- **Port and Service Enumeration [HTTP Service]**
- **Exploitation of Gym Management System [Unauthenticated RCE]**
- **Post-Exploitation Evaluation with winPEAS [SMB Service]**
- **Port Forwarding Configuration with Chisel [8888:127.0.0.1:8888]**
- **CloudMe Exploitation: Buffer Overflow [Debugging and Python Scripting]**

Ethical hacking lab: Buff HackTheBox

>- Doble extensión .php.png: Se refiere a una técnica de evasión donde un archivo tiene una doble extensión (por ejemplo, malicious.php.png). Aunque la extensión visible es .png, que es una extensión de imagen, el archivo puede estar diseñado para ser tratado como un archivo .php en un servidor web, lo que puede permitir la ejecución de código PHP malicioso.

>-RCE sin autenticación (Remote Code Execution): Es una vulnerabilidad de seguridad que permite a un atacante ejecutar comandos o código en un sistema de forma remota sin necesidad de autenticarse. Es una amenaza crítica porque puede dar acceso completo al sistema afectado.

>-Searchsploit: Es una herramienta de línea de comandos que permite buscar y mostrar exploits y vulnerabilidades en la base de datos de Exploit-DB. Es útil para encontrar posibles vulnerabilidades que se puedan utilizar en una evaluación de seguridad.

>-Función shell_exec: Es una función en PHP que permite ejecutar comandos del sistema operativo desde un script PHP. Puede ser utilizada para ejecutar comandos shell en el servidor, lo que puede ser riesgoso si se usa de manera insegura.

>-Netcat: Es una herramienta de red que puede leer y escribir datos a través de conexiones de red utilizando los protocolos TCP o UDP. A menudo se utiliza para crear shells reversas o para establecer conexiones de red básicas para pruebas de penetración.

>-WinPEAS: Es una herramienta de enumeración de privilegios en sistemas Windows. Ayuda a identificar configuraciones inseguras, permisos de archivos, y otras posibles escalaciones de privilegios en sistemas Windows.

>-Chisel: Es una herramienta para hacer port forwarding o tunneling sobre HTTP. Permite redirigir tráfico de red entre diferentes sistemas a través de un túnel HTTP, lo cual puede ser útil para acceder a servicios internos o restringidos.

>-Reverse Shell: Es una shell que se establece desde un sistema comprometido a un sistema atacante. En lugar de que el atacante se conecte al sistema comprometido, el sistema comprometido establece una conexión de vuelta al atacante, permitiendo al atacante ejecutar comandos y obtener acceso al sistema.

>-Sobrescribir el registro EIP: En un ataque de buffer overflow, el registro EIP (Instruction Pointer) puede ser sobrescrito para redirigir la ejecución del código a una dirección específica, como una dirección que contiene código malicioso. Esto es clave para explotar vulnerabilidades de desbordamiento de búfer.

>-Buffer Overflow (Desbordamiento de búfer): Es una vulnerabilidad que ocurre cuando un programa escribe más datos en un búfer de los que este puede manejar. Esto puede sobrescribir datos adyacentes en la memoria, permitiendo a un atacante ejecutar código malicioso o causar fallos en el programa.

>-Immunity Debugger: Es una herramienta de depuración para sistemas Windows que permite analizar y depurar aplicaciones. Se utiliza para identificar vulnerabilidades, como el sobrescribir registros en la pila durante un ataque de buffer overflow.

>-Pila (Stack): Es una estructura de datos en la memoria que sigue el principio LIFO (Last In, First Out). En el contexto de seguridad, la pila se usa para almacenar direcciones de retorno y variables locales. Manipular la pila puede llevar a la ejecución de código malicioso.

>-Port Forwarding (Redirección de puertos): Es el proceso de redirigir el tráfico de una red desde un puerto en un sistema a otro puerto en un sistema diferente. Esto es útil para acceder a servicios que están detrás de un firewall o en una red privada.

>-Lenguaje C: Es un lenguaje de programación de propósito general muy utilizado en sistemas y desarrollo de software de bajo nivel. Es conocido por su eficiencia y control sobre el hardware.

>-Msfvenom: Es una herramienta de Metasploit que se utiliza para generar payloads (código malicioso) para diversas plataformas. Permite crear payloads personalizados que se pueden utilizar en pruebas de penetración para explotar vulnerabilidades y obtener acceso a sistemas